



ELECTRONIC CASH CONTROLLED BY
NON-HOMOMORPHIC SIGNATURES

5

Background Of The Invention

Field Of The Invention

The present invention generally relates to a method and system to create and manage
10 digital cash.

Prior Art

A review of digital cash and other forms of electronic payment systems can be found
in D. O'Mahony, M. Peirce, and H. Tewari: Electronic Payment Systems (Artech
15 House, Boston, 1997). The basic idea of electronic cash is that a digitally signed
statement of value from a bank can be redeemed by the bank as no one else can
produce such a statement, as long as the bank keeps track of the statements it has
already redeemed. To protect the beneficiary of the statement, encryption will be used
in communication, or the delivery has to be made by conventional delivery methods.
20 This basic principle however does not allow for anonymity, which is often considered
as one of the main virtues of cash. To overcome this difficulty, David Chaum (D.
Chaum "*Blind Signature System*", Advances in Cryptology: Proceedings of Crypto 83,
Plenum Press, New York, 1984, Pages 153—153) has proposed to use blind signature,
which uses the homomorphic property of the RSA protocol for public signature.

25

This idea has been the starting point of actual use of electronic cash, as offered by the
Mark Twain Bank of St. Louis, Missouri for some time starting October 1995. The
fact that this operation was not continued is most probably due to the fact that
electronic commerce (or e-commerce) was not yet developed enough. The growth of
30 e-commerce as we witness it now will certainly ask for some forms of electronic cash
to be available. It is thus important to provide ways to generate and manage electronic

cash which would have all the virtues, and avoid the weaknesses, of the solutions originally offered.

One approach to address this need is to use a digital signature Sign . The main property of a digital signature Sign such as RSA which is used for blind signatures is

5 the fact that Sign has some interesting algebraic properties:

1) it is a homomorphism, i.e., $\text{Sign}(kx) = \text{Sign}(k)\text{Sign}(x)$,

2) it is possible to create pairs $r, \text{Sign}(r)$

for a random message r . More precisely, anyone can choose $\text{Sign}(r)$ at random and then compute r as the function Sign^{-1} is known publicly.

10

The basic idea is as follows. Customer C will choose a message x which is going to be the coin. Also, C will generate a pair $k, \text{Sign}(k)$, for a random number k . C sends the product kx to the bank B which will compute $\text{Sign}(kx)$. B then sends $\text{Sign}(kx)$ to C , using, for instance, a public encryption scheme provided by C , or using some
15 session key exchanged between C and B using a Diffie-Hellman session, or using some other form of communication such as delivery on a diskette transported by an armored carrier. C can then compute $\text{Sign}(x)$ by simply dividing $\text{Sign}(kx)$ by $\text{Sign}(k)$. The pair $(x, \text{Sign}(x))$ is now redeemable by B , at a value usually determined by the signature being used, and B cannot recognize C when some payee P presents $(x, \text{Sign}(x))$, as the knowledge of kx does not allow practical recognition of x nor of
20 $\text{Sign}(x)$.

The main problem with the approach described above is that a signature scheme with properties (1) and (2) described above is clearly not secure. Indeed property (2) says
25 that it is easy to forge signatures on random messages. Property (1) says that after seeing the signatures on two messages x_1 and x_2 , it is easy to compute the signature on the message $x = x_1x_2$. In order to overcome this problem, valid messages are required to have a special "structure" (e.g., the message x must be encoded using the PKCS#1 standard for digital signature). The hope is that messages with this structure
30 are sparse and hard to forge even given properties (1) and (2) (since messages with

that structure will not appear with a significant probability). However, this is simply a hope and is not a proven mathematical property of the signature scheme or of the encoding. The drawback is that it may be possible to discover an algorithm to forge messages even when we restrict them to this structured sparse set.

5

A *provably secure* signature scheme instead has the property that even after seeing several signed messages, it is not possible to produce a different valid message. This is a mathematical property of the signature scheme which is proven under some reasonable computational assumption (say the hardness of factoring large integers).

- 10 Provably secure schemes are known in the cryptographic literature, but for none of them is it known how to create a blinding mechanism.

Summary Of The Invention

- 15 An Object of this invention is to improve cryptography methods and systems.

Another object of the present invention is to provide a method and apparatus to create and manage electronic cash using possibly a non-homomorphic signature scheme.

- 20 A further object of this invention is to provide a mechanism to create digital cash which does not use blinding and relies on provably secure signature schemes.

Another object of the present invention is to provide a method and system to emit and circulate secure electronic cash that allows to use non-homomorphic signature

- 25 schemes, and avoids having to use blind signature techniques.

A further object of this invention is to provide a method and system to emit and circulate secure electronic cash that allows to use non-homomorphic signature schemes and avoids having to use blind signature techniques, and where the

generation of the electronic cash is performed using secure cryptographic hardware that protects its keys from everyone, including the owners.

5 These and other objective are attained with a method and system for establishing and managing digital cash. This method is to emit and circulate secure electronic cash that allows to use non-homomorphic signature schemes, and avoids having to use blind signature techniques. With one specific embodiment, the method provides anonymous digital cash, and comprises the steps of providing an entity with a secure coprocessor, a user establishing a secure channel to a program running on said coprocessor, and the
10 user sending a coin to be digitally signed to the coprocessor.

Brief Description Of The Drawings

15 The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

20 Figure 1 illustrates an IBM 4758 PCI Cryptographic coprocessor, which may be used in the practice of this invention.

Figure 2 is a block diagram that also represents the main flows needed for the preferred embodiment of the present invention.

Detailed Description Of The Preferred Embodiments

25 The present invention builds on a pair of technologies: (1) a secure cryptography generator such as the IBM 4758 PCI Cryptographic Coprocessor; and (2) Cryptography.

30 The IBM 4758 PCI Cryptographic Coprocessor:

The IBM 4758 PCI Cryptographic Coprocessor is a programmable, field upgradeable piece of secure hardware that has a general purpose computational power about equivalent to a personal computer from the early 90's. It performs high speed cryptographic operations, and provides secure key storage. It is both

5 cryptographically secure and able to detect and protect itself against physical attacks (probe, voltage, temperature, radiation). It is in fact one of the only two devices that are **Federal Information Processing Standard** (FIPS) 140-1 overall 4 certified (hardware and microcode: certificate #35), the other one coming integrated in IBM 390 mainframes (the IBM CMOS Cryptographic Coprocessor: certificate #40) while

10 the price of an IBM 4758 is about a couple of thousand dollars. The IBM 4758 is indeed a popular PCI bus interface for servers, and can serve as device driver for NT, AIX, OS/2, Linux, and OS/390.

Typical use of cryptographic coprocessors such as the IBM 4758 or some smart cards

15 include High Speed Bulk Cryptography (for instance for digital movies, in-flight entertainment systems, secure databases, confidential video-conferences, telemedicine, telecommuting, etc.) and Security in Non Trusted Environments (for instance, for smart card personalization, electronic currency dispensers, electronic benefits transfer, server-based smart card substitutes, home banking, certification authorities, secure

20 database key control, e-postage meters, electronic payments, secret algorithms, secure time stamps, contest winner selection, software usage metering, electronic securities trading, hotel room gaming, etc.).

Cryptography

25 The use of Private key/public key pairs (or SK/PK pairs; we also say public schemes) as means to encrypt or digitally sign a file or document, of secret encoding keys, and of secure hash functions (such as SHA-1, as fully specified in the Federal Information Processing Standard Publication 180-1) are now well known. A description of these techniques with directions on how to use several of their implementations can be

found in "Handbook of applied Cryptography", by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vastone, CRC Press, 1997.

To fix the ideas, we recall that a digital signature scheme is used in the form of a pair
5 of functions Sign and Sign^{-1} which are inverse of each other, i.e., for a message X to
be signed, $\text{Sign}^{-1}(\text{Sign}(X))=X$. The function Sign is kept secret, being known only to
some legitimate owner of the signature and his/her agents. The function Sign^{-1} is
known publicly, and accessible for instance through the World Wide Web (WWW),
through some agency specializing in providing PKI, or given away by the owner of the
10 pair to whoever needs to check the identity of the sender and/or that a message is
exactly as the owner intended it to be.

We also recall that a public encryption scheme is used in the form of a pair of
functions Encr and Encr^{-1} which are the inverse of each other, i.e., for a plain text X to
15 be signed, $\text{Encr}^{-1}(\text{Encr}(X))=X$. The function Encr^{-1} is kept secret, being known only
to some legitimate owner of the signature and his/her agents. The function Encr is
known publicly, and accessible for instance through the WWW or through some
agency specializing in providing PKI, or given away by the owner of the pair to
whoever wants to send the owner a secret message, or keep secret some part of the
20 message.

Probably the most often used public schemes (to generate and use a SK/PK pair in
order to allow for public encryption or digital signature) are the Rivest-Shamir-
Adleman (RSA) protocols. Several other methods could also be used (see, e.g., the
25 "Handbook of applied Cryptography"). In the case when the functions Sign and Sign^{-1}
(or Encr^{-1} and Encr) are produced according to the RSA protocol, it is now preferred
to use at least 1024 bits for X and $\text{Sign}(X)$ (the formerly often used 512 bits are no
more considered as secure).

The RSA scheme works as follows. The signer (let us call him Bob) chooses two large primes P, Q (say 512 bits long) and sets $n = PQ$. Then he chooses a small prime number e which is relatively prime to both $P-1$ and $Q-1$. This property guarantees that there exist a number d such that for any k , $k^{ed} \bmod n = k \bmod n$.

5

Bob sets (n,e) as his public key and keeps d secret as well as P and Q . The signature for a message X is $S_x = \text{Sign}(X) = X^d \bmod n$.

And it can be verified by checking that $S_x^e = X \bmod n$.

10

Clearly the RSA scheme has the homomorphic property $\text{Sign}(kx) = \text{Sign}(k)\text{Sign}(x)$.

Also it is possible to generate random pairs $(r, \text{Sign}(r))$: simply choose a random integer R smaller than n and then set

15

$$R = \text{Sign}(r), \text{ and } r = R^e \bmod n.$$

As discussed earlier, these are the properties that allow for *blind signature*.

Mathematically, the blind signature protocol using RSA works as follows. Alice wants Bob to sign message x but without him knowing that he signed it for her. This is accomplished in three easy steps:

20

1. Alice chooses a *blinding factor*, k , as a random number between 1 and n , and *blinds* x by computing $U = xk^e \bmod n$.

25

2. Bob signs U as $U^d = (xk^e)^d \bmod n = x^d k^{ed} \bmod n = x^d k \bmod n$.

3. Alice unblinds U^d by computing the signature of x as

30

$$\text{Sign}(x) = U^d / k = (x^d k \bmod n) / k = x^d \bmod n.$$

In electronic cash application, Bob is the bank B, and will need to keep track of all pairs $(x, \text{sign}(x))$ which have been redeemed. To keep databases bounded, expiration dates will be associated to any signature. Notice that in order for this to be a valid
5 blinding mechanism, x must follow some special structure (for example, follow the PKXS#1 standard for digital signatures). Pairs $(x, \text{Sign}(x))$ in which x does not follow the prescribed structure are not valid coins (otherwise Alice could easily generate coins on her own).

- 10 Golwasser, Micall, Rivest ("*A Digital Signature Scheme Secure Against Chosen-Message Attack*", SIAM J. On Computing, Vol.17, no.2, pp. 281-308); and Dwork, Naor ("*An Efficient Existentially Unforgeable Signature Scheme and Its Applications*", J. Of Cryptology, Vol.11, No.3, pp.187-208) among others, have recognized that the homomorphic property of RSA is a potential source of weakness. They also proposed
15 new signature schemes that are provably secure, i.e., in which it is provably impossible (under some reasonable computational assumption) to forge signatures. Other, more efficient, provably secure protocols have been proposed, for instance by Gennaro, Halevi, Rabin ("*Secure Hash-and-Sign Signatures Without the Random Oracle*", EUROCRYPT'99, pp. 123-139, Springer LNCS vol. 1592) or Cramer,
20 Shoup ("*Signature schemes based on the Strong RSA Assumption*", Proc. 6th ACM Conf. on Computer and Communications Security, 1999).

As a message may contain much more information than the length of the keys, several methods can be used, possibly concurrently, as is well known in the art. For instance,
25 one can split the message in several pieces, some or all of which will be signed, or one can compress the information, for instance using a secure hash function, or one can select a subset of the information, etc. Clearly, the protocol which is chosen has to be known publicly if one desires to use public key cryptography.

Notice that even if one wishes to use the benefits of public key cryptography, it may be useful to also hide secret information in the messages, so that one could recognize that someone has succeeded in breaking the keys being used. As usual in the art, it is advisable to change the keys being used every so often, depending on the application,
5 and to keep a list of former keys.

Another important enabler of secure electronic communication is the possibility to exchange secret keys while exchanging only messages which can be understood by third parties. Several protocols have been created to this effect such as Diffie-
10 Hellman.

The preferred embodiment of the present invention uses a secure cryptographic generator such as the IBM 4758 PCI Cryptographic Coprocessor to create and manage electronic cash using possibly a non-homomorphic signature scheme. Preferably, the
15 secure cryptography generator has the following properties, something which can be achieved by the 4758:

Prop1: it has a public key signature $(\text{Sign1}, \text{Sign1}^{-1})$, whose secret part Sign1 cannot be obtained by anyone, except
20 possibly by very special attacks which cannot be unnoticed, (no such attack has been proven to succeed so far on the 4758),

Prop2: it can perform standard encryption, say some list List1 of them, once provided keys to that effect; once provided an encryption scheme ES in List1 and an associated
25 key $k(\text{ES})$, and a request to sign a certificate in some prescribed format Cert , corresponding to an amount that belong to a list List2 , it will only accept to provide the signature $\text{Sign}(\text{Cert})$ after encryption using the method ES and the key $k(\text{ES})$ - the clear form of $\text{Sign}(\text{Cert})$ cannot be obtained by anyone, except by very special attacks which cannot be unnoticed (again, no such attack has been proven to succeed so far on
30 the 4758).

Some extra properties can be imposed for some embodiments of the invention, some of which will be listed later, but Prop1 and Prop2 are the basic properties we assume each time we speak of a secure cryptography generator.

5

When ordering cash, customer C communicates to the secure cryptography generator SCG at the bank B (preferably using some secure channel on which both SCG and B can read), its own public encryption scheme (method belonging to List1, and key, all together denoted as Encr2), and orders some cash amount, with a description of the way to cut the amount into units, in a way compatible with List2 (for instance List2 will comprise all amounts available with regular coins and bills in the currency of interest to the customer). Each unit, Unit, is signed by the secure cryptography generator, and the signature Sign1(Unit) is then encrypted as Encr2(Sign1(Unit)) by SCG using the customer's public encryption scheme.

15

The SCG also computes Encr2(Unit). Besides the value, Val(Unit), of the unit, and preferably an expiration date, Exp(Unit), Unit comprises a large random number generated by SCG, in such a way that the same number will never reappear in further transactions, and possibly a secret version of that number provided by SCG, using a very secure method such as a one time pad. The SCG then communicates the quadruple

20

$$(\text{Val}(\text{Unit}), \text{Exp}(\text{Unit}), \text{Encr2}(\text{Unit}), \text{Encr2}(\text{Sign1}(\text{Unit})))$$

25 to the computer system of the bank. After payment of Val(Unit) and fees, B communicates the quadruple to C, and keeps it in its database until some expiration date that C knows and accepts beforehand (unused electronic cash can be substituted back to regular cash, or to electronic cash with later expiration date, possibly for a fee). The communication from SCG to C through B allows to guarantee the delivery of the quadruple in case of crash of one of the machines involved and/or the

30

communication lines. It also allows C to ask for a copy of the quadruple if it is later lost before use.

C will later use the electronic cash by offering the pair $(Unit, Sign1(Unit))$ as payment.

- 5 The recipient of the pair can check with B the validity of the pair. Once a pair has been redeemed, Unit is kept in the database of B until expiration of its validity, to avoid repeated use by C or any other party.

- 10 Notice that when a recipient presents $(Unit, Sign1(Unit))$ to B for credit, it is not possible for B to link this signed coin to the customer C who withdrew it in the first place. Indeed at withdrawal time, all the bank B saw was the encrypted value $Encr2(Unit)$, $Encr2(Sign1(Unit))$ and this does not allow in practice recognition of the decrypted values.

- 15 Traditional electronic cash management functions, such as replacement of electronic cash coming close to expiration by an electronic wallet held at C's location can be used as with former forms of electronic cash.

The advantages of the present method comprises the following properties:

- 20 -any signature scheme, in particular provably secure ones such as Cramer-Shoup, can be used for Sign1.

-supplementary encryption, possibly more secure or more efficient than public key, can be used by the SCG, which is useful in particular for large value units,

- 25 -the same signature can be used for different amounts as Unit may allow for this freedom, within List2,

-the bank is better protected from possibly corrupt employees.

30

One of the important modifications which can be made is to use multiple signatures, provided by some set of SCGs instead of a single one. For instance, five machines could sign, and the electronic cash would be accepted as soon as three signatures at least are legitimate.

5

Besides examining the pairs (Unit, Sign1(Unit)) as unique verification, B can also be asked to accept Unit as one it has produced. This has the advantage of extra security for B. This step cannot be done if the SCG is destroyed, but identically programmed backups can be provided, and this is an extra step of security anyhow.

10

Also, although perhaps less preferred, the SCG may be authorized to print out the list of Units it has generated and their signatures using Sign1, after a sufficient number of operations have been made. In fact, several SCG's could arrange to print out their combined lists every so often.

15

With reference now to Figure 2, at 100 we have represented the customer C, at 200 we have represented the bank B, which has one or more secure cryptography generators (SCG), possibly in the form of 4758 machines, at 210, one or more databases at 220, one or more payment systems at 230, one or more computer systems at 240, at 300 we have represented some seller with whom C will want to use the electronic cash.

20

The bank acquires the SCG's from some vendor, such as IBM for the IBM 4758. The machines may have property Prop3 below, besides Prop1 and Prop2:

25

Prop3: it has a public key encryption scheme (Encr1, Encr1⁻¹), whose secret part Encr1⁻¹ cannot be obtained by anyone, except possibly by very special attacks which cannot be unnoticed (once more we recall that, so far, no such attack has been proven to succeed so far on the 4758).

30

This will allow several machines to have the same keys without the keys to be compromised. The machines can also this way share one time pads, and other cryptographic function. Instead of Prop3, the machines can also communicate by building session key, for instance using the Diffie-Hellman protocol. When we speak of a SCG, we speak either of a single machine, or a series of them working in a coordinated way, as a multi-component single machine. The invention does not depend on the distinction between these two cases.

When the customer wants to buy electronic cash from B, it composes a message 105 comprising

1. the description of the order, according to some format communicated or posted by B,
2. the public key of its own public key encryption scheme (together with the designation of that scheme: C will check that this scheme belongs to those in List1 that can be handled by the bank's SCG).

C then sends this message to the bank, and it reaches the SCG at 210.

The SCG then generates the quadruple (Val(Unit), Exp(Unit), Encr2(Unit), Encr2(Sign1(Unit))) which is stores in the database 220.

After C pays at 230, the value Val(Unit), or a collection of them, depending on the original order 105, B sends to C the pair

(Encr2(Unit), Encr2(Sign1(Unit)))

at 115. From this pair C (and C only in a reasonable time) can compute the clear pair

(Unit, Sign1(Unit))

at 125 that will later be used, e.g., with some seller at 300. When the seller, or whoever else, is proposed the pair 125 as payment, it will check validity with B. B will use computer system 240 to check the cryptographic validity of the message, and
5 database 220 to check that the Unit has not yet been used. If the pair is valid, payment is made to 300: for instance its account belonging to 300 is made. B then store Unit in the database until expiration at least.

While it is apparent that the invention herein disclosed is well calculated to fulfill the
10 objects stated above, it will be appreciated that numerous modifications and embodiments may be devised by those skilled in the art, and it is intended that the appended claims cover all such modifications and embodiments as fall within the true spirit and scope of the present invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206